Q-KYC SXM - Bestuurlijke samenvatting + nalevingskosten

Voor het toezichthoudersgesprek met FIU/MOT en CBCS

Q-KYC SXM - 4MFESW / DNFBP Tenant

2026-06-16

Table of Contents

Q-KYC SXM — Bestuurlijke samenvatting 1

1. Wat Q-KYC SXM is, in één alinea 1

2. Wat het NIET doet, in één alinea 2

3. Waarom dit van belang is voor FIU en CBCS 2

4. Defensieve ontwerpkeuzes waar de toezichthouder om geeft 2

5. Cijfers, vandaag 4

Prijzen 4

Q-KYC SXM-tarieven 4

Overige nalevingskosten (los van Q-KYC) 5

Hoe de alternatieven prijzen 5

Wat het verschil tussen niveaus daadwerkelijk is 5

Verantwoording 6

Q-KYC SXM — Bestuurlijke samenvatting

Voor: FIU/MOT en CBCS, ter voorbereiding op het toezichthoudersgesprek met the Tenant Firm (configured at install) **Van:** the Tenant Firm (configured at install), Sint Maarten **Datum:** 2026-05-31 **Systeemversie:** Q-KYC SXM v0.6.11

De Engelse editie is de gezaghebbende versie. Deze vertaling is beschikbaar voor MOT-correspondentie; verifieer bij twijfel tegen de Engelse tekst.

---

1. Wat Q-KYC SXM is, in één alinea

Q-KYC SXM is een on-premise AML/CFT-besturingssysteem voor één DNFBP. Het verzamelt cliëntidentiteits- en eigendomsgegevens, screent deze in real time tegen OFAC/UN/EU-sanctielijsten, scoort risico tegen FATF Aanbevelingen 10 en 12, genereert

toezichthouder-klare artefacten (goAML 4.0 SAR/CTR, KvK UBO-aangifte, CBCS Jaarverslag) en schrijft elke handeling weg naar een hash-geketende audit-log die niet zonder detectie achteraf gewijzigd kan worden. Het draait op één enkele Windows-machine op kantoor. De MLRO is de enige met bevoegdheid een SAR in te dienen; het systeem dwingt dat af via rol-gebaseerde toegangscontrole.

2. Wat het NIET doet, in één alinea

Q-KYC SXM dient vandaag niet automatisch in bij enige toezichthouder, omdat geen van FIU/MOT, KvK SXM of CBCS momenteel een programmatische ingang publiceert waarheen ingediend kan worden. De MLRO downloadt elk artefact en dient handmatig in via het webportaal of e-mail van de toezichthouder; de ontvangst- bevestiging wordt vervolgens terug aan de audit-keten verbonden. Q-KYC SXM is ook geen gezichtsherkennings- of liveness-detectie- dienst — die zijn voor een fase-2 Onfido/Sumsub-integratie gepland. Het verzendt geen cliëntgegevens van de kantoorpremises behalve wanneer de MLRO daarvoor kiest.

3. Waarom dit van belang is voor FIU en CBCS

Voor de **FIU**: elke SAR die de firma via goAML indient wordt voorafgegaan door een dossier dat (a) de screeningrun bevat die het triggerde, met providernaam, versie en snapshot-hash; (b) de MLRO-beslissing met tijdstempel en hash-geketend audit-spoor; (c) het SAR XML-concept zelf. Als de FIU later vraagt “hoe wist u dat dit verdacht was?”, is het antwoord reproduceerbaar uit het artefact-bundel. Tip-off-vergrendeling wordt automatisch geactiveerd zodra een SAR wordt opgesteld (Wwft art. 23).

Voor **CBCS**: het systeem genereert een eenvoudig in te dienen Jaarverslag AML/CFT dat entiteitsaantal, risicoverdeling, zaakdoorlooptijd, SAR-aantal, sanctie-treffer-aantal en de integriteit van de audit-keten samenvoegt — direct gericht op CBCS Provisions & Guidelines sectie 6 verwachtingen. Het verslag is reproduceerbaar tot elke historische datum omdat elk gegevenspunt afkomstig is uit onveranderlijke audit-events.

Voor de **AVG/GDPR-bewuste toezichthouder**: Q-KYC SXM beheert een Artikel 30 verwerkingsregister (`regulator_api_access_log`) dat elke uitlezing van cliëntgegevens door een externe toezichthouder vastlegt met de specifieke betrokkene, tijdstempel en bearer-token. De firma kan binnen vijf minuten een verzoek om inzage afhandelen.

4. Defensieve ontwerpkeuzes waar de toezichthouder om geeft

Bezorgdheid	Hoe Q-KYC SXM het adresseert
Sabotage van historische records	Hash-geketende `audit_events`-tabel; elke `event_hash` bevat de hash van de vorige rij. Elke achteraf-bewerking breekt de keten bij de volgende verificatie.
Sabotage van opgeslagen documenten	Documenten zijn Fernet-versleuteld in rust (sleutel afgeleid van JWT-secret via HKDF-

Bezorgdheid	Hoe Q-KYC SXM het adresseert
	SHA256). Plaintext SHA-256 apart opgeslagen; bij download ontsleutelt de API, hasht, en weigert te bedienen als de hash afwijkt.
Malware geüpload als cliëntdocument	Elke upload wordt door ClamAV gestreamd (3,6 miljoen signaturen, dagelijks ververst) voor schrijven naar schijf. Geïnfecteerde bestanden krijgen HTTP 422 en worden nooit bewaard.
Vervalste of vervallen ID-documenten	ICAO 9303 MRZ-parser valideert elke controle-digit op paspoorten/identiteitskaarten bij intake. Vervallen of falende documenten worden inline gemarkeerd.
MLRO-omzeiling	SAR opstellen is rol-vergrendeld; alleen `mlro` (of hoger) kan `/cases/{id}/sar-draft.xml` aanroepen. Elke geslaagde en geweigerde poging is audit-geketend.
Tip-off-delict (Wwft art. 23)	Zodra een SAR-concept wordt aangemaakt, krijgt de entiteit `tipoff_locked=true`. De SPA verbergt uitgaande communicatie tijdens deze vergrendeling. Vrijgave vereist mlro/super_admin en is zelf audit-gelogd.
Multi-jurisdictionele cliënten (FATF R.10)	Selecteren van een tweede nationaliteit op het Identiteits-tabblad verhoogt risico automatisch naar medium en annoteert het dossier voor EDD-review.
Periodieke herziening (FATF R.10)	Dagelijkse geplande taak plaatst elke entiteit met overschreden `next_review_date` in een MLRO-inbox.
Recht op vergetelheid / bewaartermijn	Bewaartermijn per regime (NOIS art. 33 = 10 jaar voor SXM); apart script wist vervallen data en logt een verwijderings-event.
Auditor-onafhankelijkheid	Rol `independent_auditor` is via een globale FastAPI-dependency read-only over elk endpoint; kan geen zaken aanmaken, records bewerken of verslagen indienen.

5. Cijfers, vandaag

- **Sanctie-records geladen**: 1.578.104 over OFAC SDN + UN Consolidated + EU Consolidated, dagelijks ververst.
- **Audit-keten-diepte**: integriteit gecontroleerd vanaf genesis tot meest recente event bij elke toezichthouder-uitlezing.
- **Versleuteling in rust**: 100% van documenten (Fernet, ~256-bit symmetrische sleutel per installatie).
- **Lockout-beleid**: 5 mislukte inlogpogingen → 15 min slot per gebruiker.
- **MFA**: verplicht voor rollen `mlro`, `tenant_admin`, `super_admin` (TOTP, secret versleuteld in rust).
- **Backup**: nachtelijke pg_dump + document-store + service-env → versleutelde zip; geteste hersteltijd RTO < 5 minuten op verse host.
- **Talen**: operator-UI + handleiding in EN / NL / FR / ES.

Prijzen

Q-KYC SXM-tarieven

De eigen tarieven van Q-KYC — een eenmalige installatie plus een abonnement. Deze staan **los** van de overige nalevingskosten van het kantoor (hardware, UPS, externe audit, MLRO-opleiding), die bestaan ongeacht welk AML-systeem u gebruikt.

Prijzen in **EUR** (contractueel). USD ter referentie tegen EUR 1 = USD 1,1540 (ECB-referentiekoers, 11 jun 2026), naar boven afgerond op de volgende USD 100.

Niveau	Actieve cliënten	Gebruikers inbegr.	Eenmalige installatie	Maandelijks	Jaarlijks
Niveau-1 — Solist	≤10	1	€1.500 (USD 1.800)	€60 (USD 100)	€720 (USD 900)
Niveau-2 — Klein kantoor	≤50	2	€2.500 (USD 2.900)	€200 (USD 300)	€2.400 (USD 2.800)
Niveau-3 — Middelgrote DNFBP / TCSP	≤500	10	€3.000 (USD 3.500)	€1.500 (USD 1.800)	€18.000 (USD 20.800)
Niveau-4+	>500	—	projectbasis	projectbasis	projectbasis

De installatiekost is exclusief hardware en externe abonnementen (bijv. cloud-opslag).

Aanbod oprichtingspilot: open voor de eerste 10 abonnees. Minimale verbintenis 6 maanden; de volledige **25% korting op het jaarabonnement** (installatie niet gekort) vereist een 3-jarige verbintenis: Niveau-1 €540/jaar · Niveau-2 €1.800/jaar · Niveau-3 €13.500/jaar.

Extra gebruikers boven het inbegrepen aantal: +€720 (Niveau-1) / +€1.200 (Niveau-2) / +€1.800 (Niveau-3) per gebruiker per jaar.

Overige nalevingskosten (los van Q-KYC)

Naast de Q-KYC-tarieven hierboven draagt een kantoor de gebruikelijke kosten van een AML-programma — een server, een UPS, off-site back-up, externe auditdagen en MLRO-bijscholing. Dat zijn de eigen operationele kosten van het kantoor en hangen af van eigen keuzes; ze zijn gelijk ongeacht welk AML-systeem u draait en vallen buiten deze samenvatting.

Hoe de alternatieven prijzen

De cloud-SaaS-alternatieven publiceren geen enterprise-prijzen. **ComplyAdvantage** publiceert enkel een Starter-niveau (vanaf USD 99/maand, ≤2.000 entiteiten); enterprise is op offertebasis. **Napier** en **Quantexa** publiceren in het geheel geen prijzen — beide enkel enterprise contact-sales. Alle drie zijn cloud-only en verzenden cliëntdata van het eiland af. Q-KYC publiceert de volledige prijs (hierboven), draait on-premise, en houdt elke byte binnen de jurisdictie SXM.

Wat het verschil tussen niveaus daadwerkelijk is

Regel	Niveau-1	Niveau-2	Niveau-3
Hardware	Refurb mini-PC (Intel NUC i5 / equiv.)	Mini-PC i5, 16 GB RAM, 512 GB	Mini-PC i7, 32 GB RAM, 1 TB
UPS	600 VA	1000 VA	1500 VA
Externe backup	1 TB USB	2 TB USB	4 TB USB
Initiële MLRO-training	2 uur remote	4 uur hybride	8 uur on-site
Migratie	Inbegrepen (≤20 records CSV)	Inbegrepen (≤100 records)	Apart geoffereerd >100
Cloud-backup quota	10 GB	25 GB	50 GB
Jaarlijkse audit-omvang	Zelf-attestatie + Q-KYC-integriteitscheck	Volledige externe audit, ~1 dag	Volledige externe audit, 2-3 dagen
MS365 SMTP-relais	0 (persoonlijke mailbox + app-password)	1 service-mailbox	1 service-mailbox + ticketing

Wat in **alle drie niveaus identiek is** (geen concessie aan regulatoire substantie):

- ClamAV-scan op elk geüpload bestand
- Fernet-versleuteling in rust
- ICAO 9303 MRZ-validatie
- Hash-geketende audit-log
- OFAC + UN + EU sanctielijsten, dagelijks ververst
- Tip-off-vergrendeling bij SAR-concept
- Rol-gebaseerde toegang met MFA op gevoelige rollen
- AVG Artikel 30-register op elke toezichthouder-pull
- 4-talige operator-handleiding (EN/NL/FR/ES)

U krijgt **niet minder compliance** door een kleiner niveau te kiezen; u krijgt dezelfde software op minder hardware met minder auditdagen.

Verantwoording

- **Valuta:** Q-KYC-tarieven zijn in EUR (contractueel); USD ter referentie tegen EUR 1 = USD 1,1540 (ECB-referentie, 11 jun 2026), naar boven afgerond op de volgende USD 100.
- **Prijzen:** de oprichtingspilot-korting (eerste 10 kantoren, 3-jarige verbintenis, 25% korting op het jaarabonnement, minimaal 6 maanden) is de enige korting; de installatiekost wordt niet gekort. Niveau-4+ (>500 cliënten) is op projectbasis.
- **PEP-data-noot:** de gratis OFAC/UN/EU-stack dekt al sanctie-screening; commerciële PEP-feeds zijn een *kwaliteits*- upgrade, geen *compliance*-vereiste onder CBCS P&G.

Deze samenvatting is reproduceerbaar uit het bron-markdown via de pandoc + Word-toolchain die ook de explainer-handleiding gegenereerd heeft.